ELSEVIER

Discrete Mathematics 240 (2001) 13–19

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Bounds on codes over an alphabet of five elements ☆

Galina T. Bogdanova[a], Patric R.J. Östergård[b,*]

[a] *Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, P.O. Box 323, 5000 V. Tarnovo, Bulgaria*

[b] *Department of Computer Science and Engineering, Helsinki University of Technology, P.O. Box 5400, 02015 HUT, Finland*

Received 21 September 1999; accepted 14 August 2000

Abstract

We consider the problem of finding bounds and exact values of $A_5(n,d)$ — the maximum size of a code of length n and minimum distance d over an alphabet of 5 elements. Using a wide variety of constructions and methods, a table of bounds on $A_5(n,d)$ for $n \leqslant 11$ is obtained.

Keywords: Code construction; Error-correcting code; q-ary code

1. Introduction

Let Z_q denote an arbitrary set of $q \geqslant 2$ elements, here $\{0,1,\ldots,q-1\}$, and let Z_q^n be the set of all n-tuples (vectors) over Z_q. If we explicitly use the q elements of the finite field of order q, we denote the set by F_q and the set of n-tuples by F_q^n.

We call any nonempty subset C of Z_q^n a q-ary code of length n. The vectors of C are called codewords. The minimum distance of a code, denoted by d, is the smallest Hamming distance between any pair of codewords. A q-ary code of length n, minimum distance d, and cardinality M is called an $(n,M,d)_q$ code, and if the code is linear with $M = q^k$ codewords, it is called an $[n,k,d]_q$ code.

A central problem in coding theory is to optimize one of the parameters n, M, and d for given values of the other two. The usual version of the problem is to find the largest code given the length n and the minimum distance d. We denote the largest value of M by $A_q(n,d)$. An $(n,A_q(n,d),d_q)$ code is called *optimal*.

Especially the binary case has attracted a lot of interest along the years; a table of bounds on $A_2(n,d)$ is given in [6] with some improvements in [14,17]. The ternary

☆ This work was partially supported by UNESCO UVO-ROSTE contract No. 875.630.9. and by the Academy of Finland.

* Corresponding author.

E-mail addresses: lpmivt@vt.bia-bg.com (G.T. Bogdanova), patric.ostergard@hut.fi (P.R.J. Östergård).

0012-365X/01/$ - see front matter
PII: S0012-365X(00)00383-6

case with tables on $A_3(n,d)$ has been studied in [5,20], and recently also the quaternary case has been investigated [2]. We here continue this work and present results for $q=5$. Some work on *linear* codes with $q=5$ has earlier been carried out [3,7]; tables of bounds on linear codes can be found in [4].

The paper is outlined as follows. In Section 2, we discuss some combinatorial results including a recent theorem that for $M<2q$ gives all parameters for which $A_q(n,d)=M$. In Section 3, we present several methods that have been used to find codes and thereby lower bounds on $A_5(n,d)$. The new codes obtained by the various methods are listed. Finally, in Section 4, we give a table of $A_5(n,d)$ for $n\leqslant 11$.

2. Some general bounds and optimal codes

Since $A_q(n,1)=q^n$ and $A_q(n,2)=q^{n-1}$, we study codes with $d\geqslant 3$. Some other obvious facts are given by the following theorem.

Theorem 1. (i) $A_q(n,n)=q$,
(ii) $A_q(n-1,d-1)\geqslant A_q(n,d)$,
(iii) $A_q(n,d)\leqslant qA_q(n-1,d)$.

The Plotkin bound gives good upper bounds when the minimum distance is close to the code length. Its q-ary form is as follows [2].

Theorem 2. *If there exists an* $(n,M,d)_q$ *code, then*

$$M(M-1)d\leqslant 2n\sum_{i=0}^{q-2}\sum_{j=i+1}^{q-1}M_iM_j,$$

where $M_i=\lfloor (M+i)/q\rfloor$.

The juxtaposition construction can be used to get infinite families of codes.

Theorem 3. *If there exists an* $(n,M,d)_q$ *code, then there exists an* $(\lambda n,M,\lambda d)_q$ *code for any integer* $\lambda\geqslant 1$.

By combining the Plotkin bound with a constructive result — a construction that uses juxtaposition, a result by Baranyai, and a result showing a connection between resolvable pairwise balanced designs and equidistant codes — the following result is proved in [2].

Theorem 4. *Let* $q<M\leqslant 2q$. *Then an* $(n,M,n-\lambda)_q$ *code exists if and only if* $n/\lambda\leqslant M(M-1)/2(M-q)$. *For* $M\neq 2q-1$ *equality implies that such a code is optimal.*

The theorem can also be presented in another form.

Corollary 1. *For* $q \leqslant M < 2q$, $A_q(n,d) = M$ *exactly when*

$$\frac{(M+1)^2 - 3(M+1) + 2q}{(M+1)^2 - (M+1)} n < d \leqslant \frac{M^2 - 3M + 2q}{M^2 - M} n.$$

We get the following results when $q = 5$.

Theorem 5. $A_5(n,d) = 5$ *precisely when* $\frac{14}{15}n < d \leqslant n$. $A_5(n,d) = 6$ *precisely when* $\frac{19}{21}n < d \leqslant \frac{14}{15}n$. $A_5(n,d) = 7$ *precisely when* $\frac{25}{28}n < d \leqslant \frac{19}{21}n$. $A_5(n,d) = 8$ *precisely when* $\frac{8}{9}n < d \leqslant \frac{25}{28}n$. $A_5(n,d) = 10$ *when* $\frac{48}{55}n < d \leqslant \frac{8}{9}n$.

More optimal codes can be obtained using the following theorem [19], whose generalization is used in [2] in the proof of our Theorem 4.

Theorem 6. *If there exists a* 2-(v,k,λ) *resolvable balanced incomplete block design* (*RBIBD*) *with r parallel classes, then there exists an optimal equidistant* $(r, v, r-\lambda)_{v/k}$ *code.*

Theorem 7. *Let* $\lambda \geqslant 1$. *Then* $A_5(7\lambda, 6\lambda) = 15$ *and* $A_5(6\lambda, 5\lambda) = 25$.

Proof. Theorem 6 applied to 2-$(15,3,1)$ and 2-$(25,5,1)$ RBIBDs [9] gives $(7,15,6)_5$ and $(6,25,5)_5$ codes, respectively. Applying the juxtaposition construction (Theorem 3) gives infinite families, and optimality follows from the Plotkin bound (Theorem 2). □

3. Code constructions

We will now look at constructions that can be used to get lower bounds on $A_5(n,d)$. The three constructions presented give codes from Hamming codes, codes that consist of orbits of words under the action of a permutation group, and codes that consist of cosets of a linear code, respectively. Good codes obtained are also listed. Computer search plays a central role in several of these constructions.

3.1. Codes from Hamming codes

Hamming codes are optimal q-ary codes with minimum distance 3. Hamming codes can also be used to get good q'-ary codes of the same length with $q' < q$. Notice that the construction to be presented can be applied to any code, not only Hamming codes. The first thorough discussion of the approach appears in [15]; the construction has later been used, for example, in [10,13].

For a given coordinate of an $(n,M,d)_q$ code, there must be a subset of q' different coordinate values so that the number of codewords with these values in the position is at least $q'M/q$. We now pick up these codewords, and carry out the same procedure for all other coordinates of the original code, always choosing a set of q' coordinate values that maximizes the size of the subcode.

In this process, we clearly get an $(n,M',d)_{q'}$ code with $M' \geqslant M(q'/q)^n$, and by starting from a $(q+1,q^{q-1},3)_q$ Hamming code, where q is a prime or a prime power, we obtain $A_{q'}(q+1,3) \geqslant q'^n/q^2$. By explicit analysis of Hamming codes, it is possible to improve on this bound slightly in many cases. The following result, which is proved in [15, Theorem 7], gives one such improvement.

Theorem 8. *Let q be an odd prime. Then $A_{q-2}(q+1,3) \geqslant ((q-2)^{q+1}+2^q(q-2))/q^2$.*

Several other similar results are also presented in [15], to which we refer the interested reader. Theorem 8 gives one best known lower bound in our study, namely $A_5(8,3) \geqslant 7985$. By explicitly constructing subcodes of Hamming codes, we further get $A_5(9,3) \geqslant 31040$ (but the bound $A_5(10,3) \geqslant 121340$, which is obtained in the same way, can be improved by other methods).

3.2. Cyclic codes

Many of the best known codes with a large minimum distance have a symmetry generated by a single permutation. (More general permutation groups were not considered in this work.) If this permutation consists of a single cycle, the code is called *cyclic*. A code may have one or several fixed coordinates on which the permutation does not act.

In searching for codes with the aforementioned symmetries, we first fix the permutation group and the parameters n and d, and then transform the search problem into an instance of the *maximum-weight clique problem*.

The orbits of words under the action of the permutation group become the vertices of a graph, discarding orbits that contain words with mutual distance less than d. The weight of a vertex is the length of — that is, the number of vertices in — the corresponding orbit. Finally, an edge is inserted between two vertices iff all words in one orbit are at a distance greater than or equal to d from the words in the other orbit.

The instances of the maximum-weight clique problem were solved exactly using the program *wclique* [16]. For each code in the following list, we give the base blocks on which the permutation acts. The permutation is indicated by the parentheses.

$A_5(7,5) \geqslant 53$: (101010)0, (130130)1, (222222)4, (231231)0, (240240)3, (322431)2, (324200)0, (333333)3, (334121)4, (410410)2, (422340)1, (423211)3, (443020)4, (444444)0.

$A_5(9,7) \geqslant 41$: (00000000)4, (11111111)1, (13212400)0, (14423020)1, (22222222)2, (22431410)4, (33333333)0, (34042110)2, (41204120)3, (44444444)0.

In some instances, where a group generated by a single permutation leads to a maximum-weight clique instance that cannot be solved within reasonable time, we tried to impose also the following symmetry: if c is a codeword, then so is $c+\mathbf{1}$ ($\mathbf{1}$ is the all-one word), $c+\mathbf{2}$, $c+\mathbf{3}$, and $c+\mathbf{4}$. This approach leads to the following lower bounds.

$A_5(8,5)\geqslant 160$: (11013200), (13424300), (14314010), (43302000).
$A_5(8,6)\geqslant 45$: (00000000), (21331200).
$A_5(9,6)\geqslant 135$: (143040200), (204034100), (320230000).

3.3. A matrix construction

In addition to the symmetries discussed in the previous subsection, a code may have a more general translational symmetry. With such a symmetry, a code is a union of cosets of a linear codes. The following construction gives such codes [13,18].

Let $A=[a_1\ a_2\ \cdots\ a_n]$ be an $r\times n$ matrix with column vectors a_i from F_q^r, and let $S\subseteq F_q^r$. For two words $x,y\in F_q^r$ we define the *distance between x and y using A* as $d_A(x,y)=\min\{wt(t)\,|\,At=x-y,\ t\in F_q^n\}$. If $At=x-y$ has no solution, then $d_A(x,y)=r$. We further define $d_A(S)=\min_{s,s'\in S,s\neq s'}d_A(s,s')$. The construction is now as follows [18, Theorem 1].

Theorem 9. *Let A be a parity check matrix for a linear code with minimum distance d'. Then the code $W=\{w\in F_q^n\,|\,Aw\in S\}$ has minimum distance* $\min\{d_A(S),d'\}$.

Matrices A and sets of vectors S that lead to good codes can be found by computer search; see [5] for details.

We now list the codes found in this work. For all these codes, the matrix A contains the columns of the $r\times r$ identity matrix. The column vectors in A are given first, with the vectors of the identity matrix omitted. The words in S are given after the semicolon.

$A_5(10,3)\geqslant 125000$: 1100, 2100, 1010, 1001, 1111, 4411; 0134, 1342, 2022, 2410, 3140, 3331, 4213, 4404.

$A_5(11,3)\geqslant 468750$: 1100, 1010, 2101, 2011, 4221, 1222, 4222; 1030, 1243, 2144, 2431, 3012, 4413.

$A_5(7,4)\geqslant 250$: 11100, 32100; 00001, 04444, 11324, 12410, 23223, 24300, 30134, 31212, 42033, 43111.

$A_5(8,4)\geqslant 1125$: 11100, 11010, 10101; 00134, 03343, 04211, 11422, 23224, 24142, 31030, 32403, 40300.

$A_5(9,4)\geqslant 3750$: 11100, 32100, 10011, 30021; 04340, 12414, 22333, 23102, 30042, 31221.

Table 1
Bounds on $A_5(n,d)$ for $n \leqslant 11$[a]

$n \setminus d$	3	4	5	6	7	8	9	10	11
3	5								
4	25	5							
5	125	25	5						
6	625_a^h	125_g	25_r	5					
7	2291^l 1597	554^h 250_m	125 53_y	15_r^p	5				
8	9672^l 7985_b	2291 1125_m	554 160_z	75 45_z	10^p	5			
9	44642^l 31040_c	9672 3750_m	2291 625	375 135_z	50 41_y	10_t	5		
10	217013^l 125000_m	44642 15625	9672 3125	1875 625	250 125	50 25	7_t^p	5	
11	1085069^h 468750_m	217013 78125_d	44642 15625_e	9375 3125_e	1250 625_f	250 125_f	35 25_j	6_t^p	5

[a]Unmarked bounds are from Theorem 1.
Lower bounds: a — Hamming code; b — from $(n-1)$-ary Hamming code (Theorem 8); c — from $(n-1)$-ary Hamming code (Section 3.1); d — from $[26,22,4]_5$ linear code [4]; e — from $[12,6,6]_5$ extended quadratic residue code [1]; f — from $[12,4,8]_5$ linear code [3]; g — linear code [12]; j — from $(12,25,10)_5$ code (Theorem 7); m — matrix construction (Section 3.3); r — from RBIBD (Theorem 6 and [9]); t — Theorem 4; y — cyclic code (Section 3.2); z — cyclic code and its translates (Section 3.2).
Upper bounds: h — Hamming bound [11]; l — linear programming bound [8]; p — Plotkin bound (Theorem 2).

4. A table for $A_5(n, d)$

We investigate codes of length $3 \leqslant n \leqslant 11$ and minimum distance $3 \leqslant d \leqslant 11$, and give best known upper and lower bounds — or the exact value if these coincide — in Table 1.

If only one number occurs in a position of Table 1, then this number is the exact value of $A_5(n,d)$ and the corresponding codes are optimal. If two numbers are given, the upper one denotes the best known upper bound, and the lower one the best known lower bound.

The upper bounds follow from the Plotkin bound, from the linear programming bound [8], and from the Hamming bound [11]. The lower bounds follow from the constructions in the paper and from results in the literature.

References

[1] E.F. Assmus, Jr., H.F. Mattson, Jr., On weights in quadratic-residue codes, Discrete Math. 3 (1972) 1–20.

[2] G.T. Bogdanova, A.E. Brouwer, S.N. Kapralov, P.R.J. Östergård, Error-correcting codes over an alphabet of four elements, Des. Codes Cryptogr., to appear.
[3] I. Boukliev, S. Kapralov, T. Maruta, M. Fukui, Optimal linear codes of dimension 4 over F_5, IEEE Trans. Inform. Theory 43 (1997) 308–313.
[4] A.E. Brouwer, Bounds on the size of linear codes, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Elsevier, Amsterdam, 1998, pp. 295–461.
[5] A.E. Brouwer, H.O. Hämäläinen, P.R.J. Östergård, N.J.A. Sloane, Bounds on mixed binary/ternary codes, IEEE Trans. Inform. Theory 44 (1998) 140–161.
[6] A.E. Brouwer, J.B. Shearer, N.J.A. Sloane, W.D. Smith, A new table of constant weight codes, IEEE Trans. Inform. Theory 36 (1990) 1334–1380.
[7] R.N. Daskalov, T.A. Gulliver, Bounds on minimum distance for linear codes over GF(5), Appl. Algebra Eng. Comm. Comput. 9 (1999) 547–558.
[8] P. Delsarte, Bounds for unrestricted codes, by linear programming, Philips Res. Rep. 27 (1972) 47–64.
[9] S. Furino, Y. Miao, J. Yin, Frames and Resolvable Designs: Uses, Constructions, and Existence, CRC Press, Boca Raton, 1996.
[10] H.O. Hämäläinen, Two new binary codes with minimum distance three, IEEE Trans. Inform. Theory 34 (1988) 875.
[11] R.W. Hamming, Error detecting and error correcting codes, Bell System Tech. J. 29 (1950) 147–160.
[12] R. Hill, Optimal linear codes, in: C. Mitchell (Ed.), Cryptography and Coding II, Oxford University Press, Oxford, 1992, pp. 75–104.
[13] G.A. Kabatyanskii, V.I. Panchenko, Unit sphere packings and coverings of the Hamming space, Probl. Peredach. Inform. 24(4) (1988) 3–16. (English translation in Probl. Inform. Trans. 24 (1988) 261–272) (in Russian).
[14] M. Kaikkonen, Codes from affine permutation groups, Des. Codes Cryptogr. 15 (1998) 183–186.
[15] J.G. Kalbfleisch, R.G. Stanton, J.D. Horton, On covering sets and error-correcting codes, J. Combin. Theory 11 (1971) 233–250.
[16] P.R.J. Östergå rd, wclique.c [C program; online], available at ⟨URL:http://www.tcs.hut.fi/~pat/wclique.html⟩.
[17] P.R.J. Östergård, T. Baicheva, E. Kolev, Optimal binary one-error-correcting codes of length 10 have 72 codewords, IEEE Trans. Inform. Theory 45 (1999) 1229–1231.
[18] P.R.J. Östergård, M.K. Kaikkonen, New single-error-correcting codes, IEEE Trans. Inform. Theory 42 (1996) 1261–1262.
[19] N.V. Semakov, V.A. Zinov'ev, Equidistant q-ary codes with maximal distance and resolvable balanced incomplete block designs, Probl. Peredach. Inform. 4(2) (1968) 3–10 (in Russian).
[20] R.J.M. Vaessens, E.H.L. Aarts, J.H. van Lint, Genetic algorithms in coding theory — A table for $A_3(n,d)$, Discrete Appl. Math. 45 (1993) 71–87.